第３回　重点課題検討タスクフォース　議事概要

１．日時　平成２８年２月３日（水）　１９：００～２１：００

２．場所　経済産業省別館１階１０１－２共用会議室

３．出席者（敬称略）

構成員：松本勉（座長）、上原哲太郎、太田和夫、菊池浩明、近澤武、手塚悟、松本泰、満塩尚史、盛合志帆

事務局：総務省（大森一顕、筒井邦弘、丸橋弘人、今野孝紀）、経済産業省（瓜生和久、上坪健治、中野辰実、中村博美）、情報通信研究機構（大久保美也子）、情報処理推進機構（神田雅透）

４．配布資料

（資料番号）	（資 料 名）
資料１	第 2 回議事概要（案）
資料２－１	暗号アルゴリズムの脆弱性に関する情報発信フローについて
資料２－２	暗号アルゴリズムの脆弱性に関する情報発信フロー（案）
資料３	暗号プロトコルのセキュリティ確保に向けた活動案
資料４	重点課題検討タスクフォースの来年度以降の検討課題（案）
参考資料１	急激な安全性の低下時における CRYPTREC の対応について(2011 年度第 1 回暗号技術検討会　資料 2　別紙 1)
参考資料２	暗号技術検討会　2015 年度　報告書　目次（案）

５．議事概要

１　開会

事務局から開会の宣言があった。

２　議事

議事を進めるにあたり、配布資料の説明が行われた。その後、前回会合の議事概要について、確認が行われた。

（１）暗号アルゴリズムの脆弱性に関する情報発信フローについて

資料 2-1、2-2 に基づき、事務局より説明が行われ、暗号アルゴリズムの脆弱性に関する情報発信フローについて基本合意され、来年度から運用されることとなった。

質疑応答は以下のとおり。

○菊池構成員　　暗号アルゴリズムの脆弱性について、何を基に情報を収集する予定であるのか。
○事務局（NICT）　　国際学会などでの発表及びウェブに公開される情報を基に、収集する。
○菊池構成員　　国際会議であれば十分な査読がなされているため一定程度信頼できる情報であるが、ウェブでの情報の信憑性を判断して収集する任を誰が負うのか。
○事務局（NICT）　　国際学会から情報収集することを主軸とする。なお、ウェブでの情報収集について専任の担当者は想定していないため、求める情報があったときにアドホックに事務局全体で対応する。
○松本座長　　暗号アルゴリズムの脆弱性情報を CRYPTREC がどのように監視し、またどのように報告してもらうかという体制上の課題である。

○手塚構成員　　英語と日本語の両方を速報として発表するのか。また、どこを対象として発表するつもりなのか。
○事務局（NICT）　　基本的には国内向けではあるが、CRYPTREC の活動を世界に発信することも望ましいと考えているため、出来る限り英語でも発信したい。
○松本座長　　少なくとも日本語で出来なければ、バイリンガルでは出来ない。まずは日本語できちんと情報発信できることが第一である。

○近澤構成員　　速報対象とするアルゴリズムは CRYPTREC 暗号リストに載っているものに限定するのか。
○太田構成員　　限定したほうがよい。人的資源の観点からみて、CRYPTREC 暗号リストに載っていない暗号アルゴリズムに対して実際に攻撃が起きた際に対応できるだけのリソースを事務局は保有しているのか。
○松本座長　　理想論と現実論は分けて議論をしたい。まずは、理想論としてどうすべきかの方向性を出したい。現実論としては、人的資源を強化するなどの対策が必要であると考えられる。
○事務局（NICT）　　事務局としては、速報対象を CRYPTREC 暗号リストに限定せず、影響度が高いと暗号技術評価委員会で判断した暗号アルゴリズムも対象と考えている。
確かに、現在の事務局体制では、公開までのフローを完遂するのには時間がかかると思うが、目標期間を設けて活動していく。また、事務局内に専門家がいない分野においては、外部の有識者に協力を仰ぎながら、信頼のおける情報源から得られる情報を発信していくことを目指す。

○上原構成員　　資料 2-1 にある A「暗号アルゴリズムの完全な危殆化による緊急対応」、B「正確で信頼性の高い情報を発信することによる過剰反応防止」、C「長期的なシステムの

安全性維持のための対策喚起」、D「対応不要」の分類を判断した結果は、速やかに公開してはどうか。特にCと判断された場合、外部からはBと判断されたが評価が難航しているため情報が出てこないのか、Cと判断されたため情報が出てこないのかがわからない。例えば、「ただいま精査しております。緊急性がある場合には追ってお知らせします。」みたいなものがあれば、あとはしばらく待っていて何もなければ大丈夫だったのだなとわかる。

○盛合構成員　　学会などでCRYPTREC暗号リストに記載されている暗号アルゴリズムの案件は毎回数件出てくるが、ほとんどが C に分類されるものである。このような案件はCRYPTRECが日頃からウォッチしていることを示すためにもB に近いC と判断したようなクリティカルな案件は早く出すべきというご意見は理解した。

○松本座長　　上原構成員の指摘は、CRYPTRECにインプットがあったことがCRYPTREC外からもわかっている場合にはその判断結果を早めに出すべきではないか、という重要な指摘である。

○事務局（NICT）　　情報分類を判断するためにもある程度日数が必要である。また、ほぼ公開する中身が決まっていても、どのように公開するかを決めることにも時間がかかる。

○手塚構成員　　情報分類は誰がどのような権限で行うことを想定しているのか。

○事務局（NICT）　　事務局で案を作成し、暗号技術評価委員会委員長と相談しながら決定していくことを考えている。難しい判断になるようであれば、暗号技術評価委員会のメール審議にかける場合もありうる。

○手塚構成員　　検討しているということをCRYPTRECが発信するということは、何か重要なことが起きたと受け取られる。CRYPTRECが注目した時点で、その情報は重要であり、さらに精査して分類して発信していく必要がある。CRYPTRECが常に情報発信する必要なはいと考える。

○事務局（総務省）　　事務局としても、CRYPTREC で発信することは重みがあるため、Bの情報のときに発信することの効果が一番高く、速報の意味があると考えている。Cの情報まで扱い、学会報告のような速報も発信されるようでは、頻度が増えるだけで、CRYPTRECの発信の重みが薄れてしまう恐れがある。

○盛合構成員　　年度末にCRYPTRECレポートあるいは暗号技術評価委員会で出すものが全て、そのたびにホームページに載るというわけではなくて、特にBかCかと迷ったようなクリティカルな問題で、Cにすると決まったものは早目に出しておくという解釈でよいか。

○上原構成員　　全てを対象とする必要はない。B か C か微妙な情報のときに、CRYPTRECとしてはどちらに近い判断をしているというのが外部からわかるといいのではないかと考える。

○松本座長　　情報精査ないし情報分類の段階で C かもしれないものについて、速報を出す、出さないという判断を１個オプションで入れるというのを追加した案はどうか。

○菊池構成員　　BかCかの分類結果は出すのか。もしそれを出すのであれば、BとCの本質は同じであるような気がしてきた。BもCも「今すぐ対応しなくてもよい」ということ

が伝わればよいものである。A は緊急対応が必要なもの、それ以外は緊急対応が不要なもの、ということさえすぐに伝われば、詳細は B も C もそれほど急ぐ必要はないのではないか。

〇松本座長　　B であっても、将来的に A になるかもしれないといった場合も考えられる。また、B でも判断に迷い、速報が出せないものは中間的な報告を出すのか、何も出さない場合もあるのか、という選択が必要となることもある。実際にやってみないとわからないこともあるため、少し修正したうえで基本的に資料の方法で実施することにしたい。

〇満塩構成員　　具体的なインシデントをみながら、もう１年かけてこのような議論を継続していくと、実態に沿ったフローとなると思う。

〇太田構成員　　速報が間違っていた場合、どこまで責任が問われるのか。

〇松本座長　　CRYPTREC は、法律に基づいて業務を行っているわけではなく、あくまでアドバイスを出すだけである。最善を尽くした結果、間違っていたのであれば、その時点で適切な形で公開すればよいと考える。

〇太田構成員　　CRYPTREC暗号リストの信頼を勝ち得るためにCRYPTRECがやるべきことと、開発会社が責任を持ってやるべきこととの区分けは今後の課題である。

〇松本座長　　基本合意ができたため、当面これで実施し、様子をみたいと思う。

（２）暗号プロトコルのセキュリティ確保に向けた活動について

資料 3 に基づき、事務局より説明が行われた。暗号技術活用委員会の WG として「暗号プロトコル課題検討 WG」を設けることとなった。対象とする暗号プロトコルについては、本日の意見を踏まえ、暗号技術評価委員会及び暗号技術活用委員会で検討することとなった。質疑応答は以下のとおり。

〇近澤構成員　　4 ページに活動案（A）（B）があり、現実としては（B）を選んだということか。

〇事務局（総務省）　(A)と(B)のどちらかを選択するという意味ではなく、(B) を中心にやっていくべきだと考えたという整理である。

〇近澤構成員　　ポータル機能は大変有益なので、必ずしも速報である必要はないが、CRYPTREC 内で持つか外で持つかは別として、必要だと考える。ポータルのような形に近づけることで、CRYPTREC が様々な方面から参照され、認められるのではないか。

〇事務局（総務省）　（A）の要素をどのような形で活動に取り込めるかは今後も活動形態の議論の中で続けていく項目だと考えている。

〇手塚構成員　　対象とする暗号プロトコルをどうするかというのが、最後は重要になっ

てくる。暗号プロトコルもたくさんあって、それらのものに全て対応するというのは大変である。まずは政府で利用している暗号プロトコルに対して、情報を出すのが理想である。電子政府のプロトコル、重要と思われる暗号プロトコルといったように対象を決めるとよいのではないか。

○事務局（IPA）　対象は、世の中で多く利用されているものは政府でも利用しているだろうという推測を踏まえて考えている。

○事務局（総務省）現時点では、強いニーズがまだ出てきていない状況であるため、一般的なプロトコルも含めて、調査していくところから始めるということが今回の提案の背景である。

○満塩構成員　実装には、プロトコル実装の他にプログラム実装があることも認識したほうがよい。プログラム実装や設定は、SIer に適切に実施してもらう必要があり、SSL/TLS 暗号設定ガイドラインのようなものはとても重要である。8 ページにあるプロトコルの複雑性を示した図の右側から検討することには賛成だが、「幅広く利用されている汎用的実用プロトコル」よりさらに右側に「実装」「設定」があり、実装や設定を対象としている組織をどうやって巻き込むかを含めて考えていくほうがよい。設定画面の解説まで CRYPTREC で作成する必要はないが、CRYPTREC が設定の方針を示し、実装の仕方などはメーカーや SIer に責任を持って実施してもらうという全体スキームができるとよい。

○盛合構成員　8 ページにおいて、「特定領域に特化して利用している実用プロトコル」「幅広く利用されている汎用的実用プロトコル」の２つのみが実際に使われていると限定して書くのは誤解を招く。「標準化された単機能プロトコル」でも実際に利用されている。

○事務局（IPA）　単機能が組み合わさって実用プロトコルになっているという意味で記載した。公開時には誤解がないように表現を修正する。

○菊池構成員　9 ページにある、暗号技術活用委員会の下の課題検討 WG と暗号技術評価委員会の下の評価 WG のそれぞれが対象とするプロトコルは異なるということか。課題検討 WG では、作成する運用ガイドラインの範囲を検討することが目的だと考えていたが、評価 WG で扱う評価対象のプロトコルも検討するのか。

○事務局（IPA）　課題検討 WG では暗号技術活用委員会が作成する運用ガイドラインの範囲や対象等を検討する。一方、評価 WG では、フォーマルメソッドや Universal Composability（汎用的結合可能性）のような安全性証明等の知識を蓄えるという方法をとる可能性と、運用ガイドラインで対象とするプロトコルについて評価することになる可能性のどちらもありうる。実際に課題検討 WG でこれをターゲットにしますというのを受けて、どちらをやるかというのを評価委員会で独自に判断をすることになる。

○菊池構成員　まだ決まっていないことは承知した。同じプロトコルのガイドラインが 2 冊出るようなことがないように、両委員会でどういうものを目指すのか十分に連携して検

討してほしい。

〇事務局（NICT）　SSL/TLS 暗号設定ガイドラインも暗号技術評価委員会と暗号技術活用委員会の両方から発行されているが、記述の観点が少し異なっており、活用委員会側の運用ガイドラインは実際の設定場面で利用できるガイドラインであり、評価委員会側のガイドラインは脆弱性がどうして起きているか等についての技術解説書という位置づけである。対象とするプロトコルが同じであっても、与える情報の観点が違う。

〇松本座長　セキュリティの技術的な解析のための詳細評価を、暗号プロトコルの設定方法の根拠に用いる考えもある。それぞれの委員会でばらばらに対応しないでほしい。

〇盛合構成員　暗号プロトコルのセキュリティ確保に向けた活動を始めていく中で、暗号プロトコル安全性評価がどういうものであり、どのように知見を蓄積していくかという部分をガイドラインとして出していくアプローチをとるのが、暗号技術評価委員会の役割である。一方、そのプロトコルをどのように安全な利用を促進していくか検討するのが暗号技術活用委員会の役割であり、両者は目的の違うガイドラインを作成している。

〇満塩構成員　両方で同じ「ガイドライン」という名称をつけることはやめたほうがよい。システム構築の現場では、指針なのか、設定書なのか等を気にするので、同じ「ガイドライン」で並べてしまうと混乱する。一方を評価レポートもしくは解説書とし、もう一方をガイドラインとする等、名称について工夫を検討してほしい。技術ガイドラインとつければまだわかるものの、ガイドラインは氾濫している言葉なので、できれば分けたほうがよい。

〇事務局（総務省）　成果物の議論を引き続きやっていく中で、何を目的にした成果物であるのかを整理し、名称についてもよく注意して考えていきたい。

〇松本座長　両委員会でうまく連携して進めてもらいたい。

（３）来年度以降の検討課題について

資料 4 に基づき、事務局より説明が行われた。来年度以降、引き続き、政府統一基準に向けた新たな CRYPTREC 成果物のあり方、社会ニーズを見据えた新規活動、情報システム全体のセキュリティ確保を意識した他団体との連携などを議論していくこととなった。
質疑応答は以下のとおり。

〇盛合構成員　ChaCha20 の安全性評価の必要性の判断というのが、来年度の議題にある。詳細について調べたところ、Chrome や google 系の TLS への実装が進んでいること、TLS1.2 以降、DTLS という規格で利用可能になっていること、及び、OpenSSH で実装が始まっていることがわかった。しかしながら、まだ絶対に実装しなければならないということになっていないため、至急評価すべきものなのかについて議論いただきたい。

〇上原構成員　TLS1.3 の現ドラフトではストリーム暗号は ChaCha20 のみで、今後実装が

必須になると思われる。想定よりも TLS1.3 の仕様の策定に時間がかかっているため、時間的な猶予はもう少しあると思うが、私としては、安全性評価の準備をしなければいけないと思っている。

〇松本座長　　4 ページ（２）政府統一基準に向けた新たな CRYPTREC 成果物の「NISC の改定方針」は何を指しているのか。
〇事務局（経産省）　　基本は NISC の政府統一基準の改定方針を指している。その他に必要なものがあれば、意見交換、CRYPTREC に対して求めるニーズなどを捉えたうえで、成果物を提供していきたい。
〇松本座長　　事務局案のとおりとしたい。

（４）２０１５年度第２回暗号技術検討会での報告事項について
参考資料 2 に基づき、事務局より説明が行われた。第 3 回タスクフォースの資料については、事務局で修正をした後、座長確認のうえ、暗号技術検討会に報告する。

（５）その他
暗号技術活用委員会委員案の変更について報告を行い、承認された。

３　閉会
松本座長から閉会の宣言があり、今年度開催を予定していた重点課題検討タスクフォースはすべて終了した旨連絡があった。

以上